EXHIBIT 1

We represent TengoInternet, Inc. ("TengoInternet"), 3300 North Interstate Highway 35, Suite 600, Austin, TX 78705, and are writing to notify you of a recent incident that may affect the security of the personal information of 1,874 Delaware residents. TengoInternet's investigation and response to this incident is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TengoInternet does not waive any rights or defenses regarding the applicability of Delaware law, the applicability of the Delaware data incident notification statute, or personal jurisdiction.

Nature of the Data Security Incident

On September 23, 2018, TengoInternet received evidence indicating an anonymous individual had accessed its database of consumer usernames and passwords for TengoInternet accounts, without authorization, in or prior to April 2018. TengoInternet had previously received similar communications from the same anonymous individual in April 2018; however, an investigation at that time, conducted with the assistance of an outside forensic investigator, determined the claims were not credible. While its investigation is ongoing, TengoInternet has no confirmation of any actual or attempted fraudulent misuse of consumer information resulting from this incident.

The types of PII relating to Delaware residents determined to be stored within the consumer database includes the consumer's name and username and password to their TengoInternet accounts. No payment card data or financial account information was affected.

Notice to Delaware Residents

On October 26, 2018, TengoInternet will begin providing notice of this incident to potentially impacted individuals. TengoInternet does not have address information for most of the consumers in the database. For those for whom address information exists, approximately 1,874 are located in Delaware. TengoInternet is instructing potentially impacted individuals to promptly change their passwords and change the passwords for any other online accounts for which they use either the same username or password. Such notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.*** Notice is being provided by electronic mail.

Other Steps Taken

TengoInternet is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, TengoInternet has notified the FBI of this incident.

TengoInternet has taken several immediate steps to protect against similar incidents in the future. Upon learning of this incident, TengoInternet quickly took steps to determine how the information may have been accessed and took steps to prevent further unauthorized access or incidents. TengoInternet has disabled inactive accounts and implemented a procedure to require password changes for all remaining accounts. As part of TengoInternet's ongoing commitment to the security of personal information in its care, TengoInternet is also working to review existing information security procedures and to implement additional safeguards to further secure the information on its systems. They are continuing to monitor their systems to ensure they are secure. TengoInternet is taking steps to enhance data security protections to protect against similar incidents in the future.

EXHIBIT A

To: CSID
Subject: RE: [TEST] Notice of Data Breach

-----Original Message-----
From: TengoInternet.com <notice@tengointernet.com>
Sent: Monday, October 22, 2018 12:42 PM
To: inaki.serrano@experianinteractive.com
Subject: [TEST] Notice of Data Breach

Experian IdentityWorks

Notice of Data Breach | TengoInternet, Inc.

==========

Dear Customer,

TengoInternet, Inc. ("TengoInternet"), is writing to notify you of an incident that may affect the security of your personal information. TengoInternet (which also includes legacy companies Nomad Networks, Airwave Adventures, and Nexu Innovations) is a WiFi service provider serving RV Resorts, campgrounds, state parks, and other venues. You are receiving this notice because you created an account to access WiFi services with one of our companies in the past and this information may have been compromised. This notification provides details of the incident, what we're doing to reduce the likelihood of a future event and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On September 23, 2018, TengoInternet received evidence indicating an anonymous individual had accessed our database of consumer usernames and passwords for TengoInternet accounts, without authorization, in or prior to April 2018. We had previously received similar communications from the same anonymous individual in April 2018; however, an investigation at that time, conducted with the assistance of an outside forensic investigator, determined the claims were not credible. While our investigation is ongoing, we have no confirmation of any actual or attempted fraudulent misuse of consumer information resulting from this incident.

What Information Was Involved? The information in our consumer database contains our consumers' names, email addresses, mailing addresses, and/or TengoInternet service usernames and passwords necessary to access the service. No payment card or other financial information was contained in our consumer database.

What We Are Doing. Information privacy and security are among our highest priorities, and we take this incident seriously. Upon learning of this incident, we quickly took steps to determine how the information may have been accessed and to prevent further unauthorized access or incidents. We disabled inactive accounts and implemented a procedure to require password changes for all remaining accounts. As part of our ongoing commitment to the security of personal information in our care, we are also working to review our existing information security procedures and to implement additional safeguards to further secure the information on our systems. We have also notified federal law enforcement.

What You Can Do. Although we have no confirmation of any actual or attempted fraudulent misuse of your information, we are instructing you to promptly change the password to your TengoInternet account if you have not done so in the last 30 days. If you have not used TengoInternet's services since prior to January 1, 2017, then your account has already been disabled, and you do not need to take any action with respect to your TengoInternet account. Whether or not your

TengoInternet account is active, you should change the password(s) for all other online accounts for which you use the same or similar username and password, or the same or similar email address and password. However, please also review the ***Steps You Can Take to Protect Your Information***, below, for additional resources you may use to protect your information.

For More Information. We recognize that you may have questions, and we are here to assist you. You can reach our dedicated assistance line at 1-800-637-1065 (toll free), Monday through Friday, 7:00 a.m. to 7:00 p.m., CST. You may also write to us at 3300 North Interstate Highway 35, Suite 600, Austin, TX 78705.

We sincerely regret any inconvenience this incident may cause. TengoInternet remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Eric B. Stumberg
Co-Founder | President
TengoInternet, Inc.

==========

Steps You Can Take to Protect Your Information

Monitor Your Accounts. Although we have no reason to believe any financial information of our customers was impacted by this incident, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity to help protect against possible identity theft or other financial loss.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. If you would like to order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. Although TengoInternet does not ask for, or collect or maintain in any way, Social Security numbers for our customers, we advise you that you have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian: PO Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com/freeze/center.html
TransUnion: P.O. Box 2000, Chester, PA 19016, 1-800-909-8872, www.transunion.com/credit-freeze
Equifax: PO Box 105788, Atlanta, GA 30348-5788, 1-800-685-1111, www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to supply the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security number; 3. Date of birth; 4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill or telephone bill; 6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); 7. If you are a victim of identity theft,

include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian: P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com/fraud/center.html
TransUnion: P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, www.transunion.com/fraud-victim-resource/place-fraud-alert
Equifax: P.O. Box 105069, Atlanta, GA 30348, 1-888-766-0008, www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by law enforcement. For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. The number of Rhode Island residents impacted by this event is unable to be determined.